SUMMARY OF INVENTION (MARKED UP)

[0016] The above-mentioned drawbacks are overcome and a practical advance is made over the prior art through the method and system of the present invention.

[0017] In a first aspect, the invention features a method for sending an email from an email sender to a recipient in a network. The method comprises the authentication of a sender and once verified, delivering the email to the recipient.

[0018] In another aspect of the invention, a method for sending the sender's email address along with a unique fingerprint key to an email management system for verification is provided. This email management system, hereinafter, is referred to as the Email Chief (see Figure 1). The Email Chief comprises one or multiple interconnected computers residing at a single or multiple locations. The method comprises a ~~secure~~ secured or non-secured communication between the email recipient's email server or client and the Email Chief for registration/authentication purposes.

[0019] In another aspect of the invention, a simple and effective method of differentiating spammers from non-spammers is provided. The method comprises verifying the sender's fingerprint key and deducting sender's anti-spam points before acknowledging the recipient's email server or client to deliver the email.

[0020] In another aspect of the invention, a system for registering email senders and issuing and verifying the said fingerprint keys and the said anti-spam points is provided. The system comprises the Email Chief for issuing and verifying the fingerprint keys, and issuing and deducting the points. The system makes available an online registration form, and when the sender completes the form, the system would issue a certain number of free (no charge) anti-spam points, hereinafter referred to as Pass Points. One or more files are available to the Email Chief for determining whether the email sender's address is registered, whether the email sender's fingerprint key is correct, and whether the email sender's points are sufficient.

[0021] In another aspect of the invention, a system for automatically inserting said fingerprint keys to the message for the sender. And for occasions where manual insertion of said fingerprint key to the sender's message is required, convenient cut-and-paste processes are provided.

[0022]
~~[0021]~~ In another aspect of the invention, a method of requesting a sender to register at the Email Chief is provided. The method comprises the steps of: 1) sender sending an email to the recipient, 2) the recipient's email server or email client communicating with the Email Chief to determine whether the sender has provided the fingerprint key in the email, 3) in cases either the sender has not provided the fingerprint key or the sender has provided an incorrect fingerprint key, the Email Chief asking the recipient's server to hold the email, and 4) the Email Chief sending a message to the sender requesting the sender to register.

[0023]
~~[0022]~~ In another aspect of the invention, a method of acknowledging delivery of the email and deducting the anti-spam points is provided. The method comprises the steps of: 1) the Email Chief checking the file to verify the sender is registered and the provided fingerprint key is correct, 2) acknowledging the recipient's email server or email client to deliver the email, and 3) deducting the appropriate anti-spam points from the sender.

[0024]
~~[0023]~~ In another aspect of the invention, a method enabling legitimate advertisers to buy advertisement points hereinafter referred to as Ad Points, from the Email Chief operator, and enabling the Email Chief operator to reward email recipients for their earned Ad Points. The method comprises the steps of: 1) advertiser purchasing Ad Points from Email Chief operator, 2) advertiser sending emails to recipient, 3) Email Chief acknowledging the recipient's server or email client to deliver the email, 4) Email Chief deducting the Ad Points from the advertiser, and 5) Email Chief operator rewarding email recipients earned Ad Points.

[0025]
~~[0024]~~ In another aspect of the invention, a system enabling email recipients to set one or more values for charging advertisers' Ad Points. The system comprises one or more records, for each email recipient, of the number of Ad Points he or she would like to charge for each email going to him or her. The system comprises the capability to deduct a fixed or varied number of points if the sender's anti-spam points are issued through the registration process; and the capability to deduct the number of points required by the recipient if the sender's anti-spam points are purchased from the Email Chief operator.

[0026]
~~[0025]~~ In another aspect of the invention, a system capable of limiting the number of email accounts from which each individual could redeem Ad Points for reward.

[0027]
~~[0026]~~ In another aspect of the invention, a system capable of increasing or decreasing, on a fixed or varied schedule, an account's Pass Points to any chosen value or range.

[0028]
~~[0027]~~ In another aspect of the invention, a system capable of catering to the language of the user during registration, or for any other interaction with the system.

[0029]
~~[0028]~~ In another aspect of the invention, a system enabling domain owners to issue anti-spam points to email users for emails delivered only to within that same domain. These domain restricted anti-spam points are hereinafter referred to as Dom Points.

[0030]
~~[0029]~~ In another aspect of the invention, a system enabling email users to ~~acquire~~ purchase anti-spam points for the safe passage of their solicited emails. These safe passage anti-spam points are hereinafter referred to as Safe Points. Safe Points are typically used by mailer sending out large quantities – quantities much larger than Pass Point accounts would allow - of solicited emails. In effect, the sender provides the recipient a guaranty that the email message would not be considered spam. Such solicited emails, for example, include periodic newsletters, responses to inquiries, and automatic notifications.

[0031] In another aspect of the invention, a system optionally providing a notification period to senders who have not registered to be notified without having their email being held up or blocked by a new user of this invention. During the notification period, senders who have not registered would receive a reminder to go register each time the Email Chief delivers their message to a new user of this invention.

[0032]
~~[0030]~~ In another aspect of the invention, a system capable of tracking registered users' email usage patterns to establish user classification.

[0033]
~~[0031]~~ The differences between prior arts and the present invention are numerous and significant.

[0034]
~~[0032]~~ 1) The present invention is not rule-based or keyword-based, thus there is no danger of filtering away an important email. It starts protecting an email user immediately after his email server or client is communicating with the Email Chief.

[0035]
~~[0033]~~ 2) There is no need to change the current email protocols~~, the only~~ - information exchanged between the email server or client and the Email Chief is the encoded string ~~containing the sender's email address and the fingerprint key~~, and the authenticating process can be easily implemented by writing a computer program to interact with both the email server or client program and the Email Chief. It is no more complex than the programs run by many email servers for filtering emails.

[0036]
~~[0034]~~ 3) With the fingerprint key, a user is protected from spammers stealing his or her identity or email address to send out spams.

[0037]
~~[0035]~~ 4) Only a one-time registration is required for the email sender. Once registered, the system will automatically replenish the anti-spam points of the email users after a fixed or varied period of time has elapsed. The number of emails permitted to be sent using the present invention within a certain period of time thus is limited, effectively distinguishing spammers from normal email users.

[0038]
~~[0036]~~ 5) The user registration process is meant to incur some cognitive costs for the email sender. Users are able to omit sensitive information if they so desire.

[0039]
~~[0037]~~ 6) The sender would need to register only once at the Email Chief for all participating email servers or email clients to verify the identity of the sender. It is much more feasible and convenient than previous solutions that require registration at each email server.

[0040]
~~[0038]~~ 7) Comparing with the challenge-response systems, the present invention does not require the recipient to build a trusted list. Once registered, a legitimate sender does not need to answer challenge questions each time he or she sends an email to a recipient who does not have his or her email address in the trusted list.

[0041]
~~[0039]~~ 8) Normal usage of sending and receiving emails would not incur any expense to the sender. High volume users could acquire Dom Points, or purchase Safe Points which are refunded if the recipient takes no action to indicate that the message is spam.

[0042]
~~[0040]~~ 9) The present invention enables the email recipients to set a personal threshold for charging Ad Points. Different people with different opportunity costs can charge different number of Ad Points and redeem them later for money, goods, and/or services.

[0043] 10) Users holding Safe Point or Ad Point accounts would use secured fingerprint keys providing high security from unauthorized use and access.

[0044]
~~[0041]~~ The present invention creates a legitimate venue for email marketing. The advertisers can buy Ad Points and set a threshold value for sending out each email. If the recipient's threshold value is lower than the advertiser's threshold value, then the email will be delivered, and if not, the email will not be delivered. For a recipient, he or she sets a threshold value according to his or her opportunity cost. If receiving the email pays him or her acceptable price, he or she is better off to read the email; on the other hand, if the email's value is lower than his or her threshold value, the email will not get through.

[0045]
~~[0042]~~ Hereinafter, an email bearing Ad Points will be referred to as Ad email. Similarly, an email bearing Dom, Free, or Safe Points will be referred to as Dom email, Free email, or Safe email, respectively.

[0046]
~~[0043]~~ There are still other differences, both major and minor, between the prior arts and the present invention. Those differences just listed, however, suffice to show that the prior arts are only marginally pertinent to the present invention. It has been useful to discuss it here, however, as the comparison highlights some of the advantages of the present invention. More advantages are discussed in the following sections.